

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-076059

(43)Date of publication of application : 23.03.2001

(51)Int.Cl.

G06F 17/60

G09C 1/00

H04L 9/32

(21)Application number : 2000-271698

(71)Applicant : MALL SERVICE:KK

(22)Date of filing : 07.09.2000

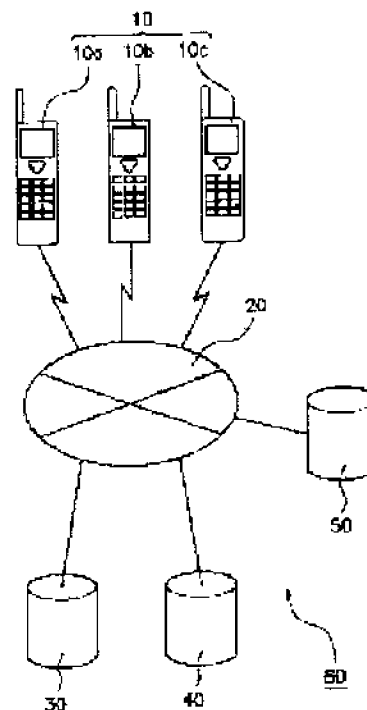
(72)Inventor : NAKA SHINICHI  
UMEMOTO YASUHIRO

## (54) SETTLEMENT SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To obtain a settlement system, which fully guarantees the security of individual information on the Internet, improves operability of a user portable terminal, consistently completes the process from commercial transaction to settlement using only the Internet, and reduces the risk of personal information being saved.

**SOLUTION:** When personal information is transmitted from a user portable terminal 10, an authentication server 30 ciphers individual information with a 1st cipher and sends it back to the user portable terminal, where the ciphered information is stored; and when an order for commercial transaction of the Internet 20 by the user portable terminal is received via an ordering destination, the personal information ciphered with the 1st cipher is sent by the authentication server, after the contents of the commerce is confirmed on the user portable terminal, the information is received, deciphered, and ciphered with a 2nd cipher and the information ciphered with the 2nd cipher is sent to a settlement server 40.



## LEGAL STATUS

[Date of request for examination] 08.11.2000

[Date of sending the examiner's decision of rejection] 16.05.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-76059

(P 2 0 0 1 - 7 6 0 5 9 A)

(43) 公開日 平成13年3月23日 (2001. 3. 23)

(51) Int. Cl.	識別記号	F I	ラマコード	(参考)
G06F 17/60	414	G06F 17/60	414	
	506		506	
	512		512	
G09C 1/00	660	G09C 1/00	660	B
H04L 9/32		H04L 9/00	673	A
審査請求 有 請求項の数 3 O L 公開請求 (全 8 頁) 最終頁に続く				

(21) 出願番号 特願2000-271698 (P 2000-271698)

(22) 出願日 平成12年9月7日 (2000. 9. 7)

(71) 出願人 500214163

株式会社モールサービス

京都府八幡市西山丸尾8-4

(72) 発明者 仲 真一

京都府八幡市西山和気18-9

(72) 発明者 梅本 康弘

京都府八幡市西山和気12-13

(74) 代理人 100074332

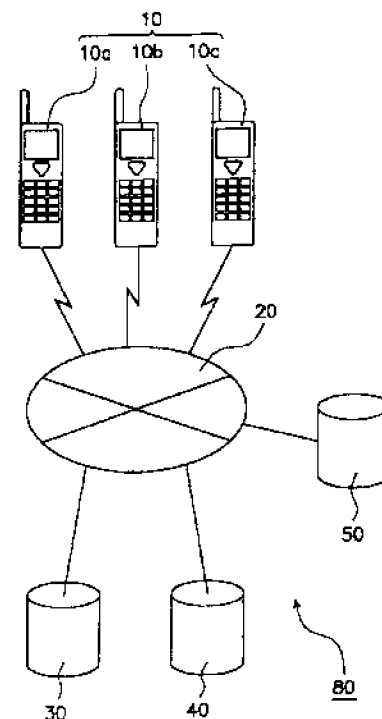
弁理士 藤本 昇 (外 2 名)

(54) 【発明の名称】 決済システム

(57) 【要約】

【課題】 インターネット上で個人情報に対するセキュリティが充分確保されるとともにユーザ携帯端末の操作性をよくし、さらには、商取引から決済に至るプロセスをインターネットのみを利用して一貫して完結できるとともに個人情報を保存するリスクを軽減できる決済システムを提供する。

【解決手段】 認証サーバ30は、ユーザ携帯端末10から個人情報が送信された場合、該個人情報を第1の暗号により暗号化して前記ユーザ携帯端末に返信して記憶させておき、前記ユーザ携帯端末によるインターネット20上での商取引の発注を発注先を介して受けた場合、前記ユーザ携帯端末に前記商取引の内容を確認させたのち前記第1の暗号による暗号化個人情報を前記認証サーバに送信させ、該情報を受信したのち復号化し、第2の暗号により暗号化し、当該第2の暗号による暗号化個人情報を決済サーバ40に送信する。



## 【特許請求の範囲】

【請求項1】 インターネットを介してユーザ携帯端末に接続された認証サーバを備え、該認証サーバはインターネットを介して決済サーバに接続されている決済システムであって、前記認証サーバは、前記ユーザ携帯端末から個人情報が送信された場合、該個人情報を第1の暗号により暗号化して前記ユーザ携帯端末に返信して記憶させておき、前記ユーザ携帯端末によるインターネット上での商取引の発注を発注先を介して受けた場合、前記ユーザ携帯端末に前記商取引の内容を確認させたのち前記第1の暗号による暗号化個人情報を前記認証サーバに送信させ、該情報を受信したのち復号化し、第2の暗号により暗号化し、当該第2の暗号による暗号化個人情報を前記決済サーバに送信し、前記決済サーバは、前記第2の暗号による暗号化個人情報を復号化して前記個人情報を認証したのち、前記認証サーバを介して前記発注先に対して前記商取引を承認して遂行させるとともに前記商取引の代金を決済することを特徴とする決済システム。

【請求項2】 前記ユーザ携帯端末は、着脱自在な記憶手段を具備し、該記憶手段は、前記第1の暗号による暗号化個人情報を記憶する請求項1記載の決済システム。

【請求項3】 前記第2の暗号は、前記第1の暗号と同一の暗号方式によるものであり、前記ユーザ携帯端末から受信した前記第1の暗号による暗号化個人情報は、前記認証サーバにおいて復号化されることなく、そのまま前記決済サーバに送信される請求項1記載の決済システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、インターネットを介して行なう決済システムに関する。

## 【0002】

【従来の技術】近年、携帯端末、特に、インターネットへの接続が可能な携帯電話等の通信手段の普及に伴い、個人ユーザが自分の携帯電話等からインターネットを介して、いわゆる電子ショップサーバ等が開設しているホームページにアクセスし、商品やサービスの内容を吟味したり、購入や契約を手軽に行なったりすること等の商取引が可能となってきている。

【0003】このような動向と相俟って、インターネットを介した商取引によって発生した商品やサービスの代金の決済を、前記電子ショップサーバの運営者も関与したかたちで銀行や信販会社等の決済機関との間で行なわれるようになってきている。ここで、個人ユーザや決済機関、該決済機関に対して個人ユーザを認証する認証機関等の間で認証や決済というプロセスが行なわれる仕組みを「決済システム」と言うものとする。

【0004】ところで、インターネットは、よく知られているように、プロバイダ等に登録してID番号やパス

ワード等の個人認証情報の付与を受けていれば、誰でも利用できるという特徴を有している。このため、インターネット自体は、個人認証情報が盗視されたり、いわゆるウイルスの感染経路となったりするなど、通信システムとしては、セキュリティ対策は、頼りにならないという状態に近いと考えられる。

【0005】そのため、前述した決済システムにインターネットを介在させようとする、以下に説明するような、セキュリティ確保のための種々の問題が生じてくる。それらは、根本的には、個人認証情報や、信販会社の発行するクレジットカードに関するカード情報等を含めた意味での個人情報の取扱いにおいて、高度化する暗号化技術を決済システム中に如何に使いやすく採り入れるか、という問題に集約されるであろうが、以下、幾つかの視点から詳細に説明する。

【0006】まず、第1に、個人ユーザの側から説明する。個人と認証機関との間、個人と決済機関との間等での認証や決済等のプロセスにおける個人情報のやり取りにおいては、前述の根本的な問題が最も端的に現われると考えられる。かかる個人ユーザの視点でのセキュリティ確保は、2つの相矛盾するような技術的要請を含んでいる。

【0007】即ち、①個人情報を暗号化する等によって、他人に盗視されたりしてもわかり難いようにし、セキュリティをより確実にしてほしいと考えることと、②実際の利用場面では、携帯電話に個人情報を入力する操作等を簡略化して利便性を高めてほしいと考えること、であり、セキュリティ確保は、この2つの技術的要請を両立させる必要があるのである。

【0008】しかし、①の要請により個人情報を暗号化等してセキュリティをより確実にしようすると個人情報自体は複雑化されることになる。即ち、個人情報が暗号化されると、これを記憶乃至は保管したり、携帯電話に入力したりする点において、個人ユーザには扱い難いものになってしまうので、そのままでは利便性があると到底言えず、②の簡略化の要請と両立し難い、ということになる。

【0009】一方、第2に、決済機関や認証機関の側の問題を説明する。従来は、認証や決済というプロセスは、セキュリティの保たれている公衆回線や特に専用回線等を利用して行なわれている。この点、インターネットを介した商取引に対しても、認証機関や決済機関、電子ショップ等の運営者等の間で行なわれる認証や決済のプロセスの殆どは、依然として、同様の公衆回線や専用回線等を介して行なわれている。

【0010】このため、インターネットを介した商取引によって発生する認証や決済のプロセスは、このプロセスを実行するための手順や実際に用いる手段に関して言えば、2種以上の通信手段を混用したものとなっており、複雑で手間のかかるものとなっている。

【0011】また、決済システム中では、決済機関以外では、ハードディスク等の内蔵記憶手段に個人情報をなるべくファイルさせたくないという要請もある。従来、認証機関や決済機関においては個人情報がファイルされており、認証や決済の都度、ファイルが参照される。個人情報がファイルされるということは、ファイルが覗かれて個人情報が漏洩してセキュリティが保たれなくなる危険性があることを意味する。

【0012】特に、多数の個人情報をファイルする立場である認証機関に対しては、ハードディスク等の内蔵記憶手段が、たとえばファイアウォール等によって防護されているのであっても、インターネット等の外部回線からアクセス可能な構造であると、決済機関としてはセキュリティ確保を特に厳しく要求し、或いは、個人情報を一切保有しないよう望んでいるというのが実状である。

【0013】因みに、決済機関の立場で言うと、個人情報をファイルするということは、例えば、個人ユーザが保有しているようなインターネットに接続可能なパソコンに内蔵されたハードディスクに個人情報を記憶させることで、外部から容易にアクセスし得る状態であるので個人情報が漏洩する危険性があるのであり、基本的に好ましくない、と考えられている程である。

【0014】このような危険性を考慮すると、決済機関の立場にしてみれば、認証機関を利用することなく自分が認証も行なうようにすれば、認証機関の介在に係るセキュリティ問題は解消するわけであるから、決済機関が認証及び決済の業務を個人ユーザ相手に直接行なうことも考えられる。

【0015】しかし、認証業務をも個人ユーザ相手に直接行なうことは、あらゆる個人ユーザから発せられるさまざまな科目や形式にわたる認証及び決済の全業務を対象とすることとなり、決済機関にとっては混乱が多くなるだけでメリットが少ないと考えられる。そこで、セキュリティを確保したうえで幾つかの認証機関によってある程度科目や形式を集約させるようにして認証機関との連携を図る方が決済システムの円滑な運営のためメリットがある、ということになりそうである。

【0016】このような事情が種々存在している従来からの慣行的実務において要求されているセキュリティを同水準で、乃至は、より高水準で、確保できる決済システム、しかも、個人ユーザによる活用が期待されるインターネットにふさわしい決済システムは未だ存在しておらず、或いは、提案されてもいない。

【0017】

【発明が解決しようとする課題】本発明は、かかる現状に鑑みてなされたものであり、インターネット上で個人情報に対するセキュリティが充分確保されるとともにユーザ携帯端末の操作性をよくし、さらには、商取引から決済に至るプロセスをインターネットのみを利用して一貫して完結できるとともに個人情報を保存するリスクを

軽減できる決済システムを提供する。

【0018】

【課題を解決するための手段】前記課題を解決するため、本発明は、インターネットを介してユーザ携帯端末に接続された認証サーバを備え、該認証サーバはインターネットを介して決済サーバに接続されている決済システムであって、前記認証サーバは、前記ユーザ携帯端末から個人情報が送信された場合、該個人情報を第1の暗号により暗号化して前記ユーザ携帯端末に返信して記憶させておき、前記ユーザ携帯端末によるインターネット上での商取引の発注を発注先を介して受けた場合、前記ユーザ携帯端末に前記商取引の内容を確認させたのち前記第1の暗号による暗号化個人情報を前記認証サーバに送信させ、該情報を受信したのち復号化し、第2の暗号により暗号化し、当該第2の暗号による暗号化個人情報を前記決済サーバに送信し、前記決済サーバは、前記第2の暗号による暗号化個人情報を復号化して前記個人情報を認証したのち、前記認証サーバを介して前記発注先に対して前記商取引を承認して遂行させるとともに前記商取引の代金を決済することを特徴とする決済システムを提供する。

【0019】かかる発明によれば、ユーザ携帯端末は、例えば電子ショップ等に商取引の発注をすると、該端末に記憶された暗号化個人情報を認証サーバから要求されて送信するので、個人ユーザは暗号化個人情報を入力する必要がない。またユーザ携帯端末には第1の暗号による暗号化個人情報が記憶されており、該個人情報は容易に解読され得ない。

【0020】従って、個人ユーザは、暗号化された複雑な個人情報を入力する必要がないのでユーザ携帯端末の操作が楽で操作性がよく、しかもユーザ携帯端末の個人情報のセキュリティが保たれている。

【0021】一方、ユーザ携帯端末から認証サーバへ、認証サーバから決済サーバへ送受信される個人情報は、それぞれ第1、第2の暗号によって暗号化されているとともに、認証サーバにおいて、第1の暗号による暗号化個人情報が復号化されるが、第2の暗号により暗号化されるので個人情報がハードディスク等の記憶媒体に保存されたりすることはなく、従って、認証サーバに個人情報が残らない。しかも商取引の発注から決済までのプロセスがすべてインターネット上で行なえる。

【0022】このように認証サーバに個人情報が残らず、従って、認証サーバ上で個人情報が漏洩するリスクが、個人情報がファイルされる場合よりも低減でき、インターネット上における個人情報の送受信に対するセキュリティも確保されている。従って、個人ユーザにとってインターネット上での商取引及び決済が安心且つ便利なものとなる。

【0023】好ましくは、前記ユーザ携帯端末は、着脱自在な記憶手段を具備し、該記憶手段は、前記第1の暗

号による暗号化個人情報を記憶する。

【0024】かかる発明によれば、暗号化個人情報を前記記憶手段に記憶させておき、前記記憶手段が着脱自在である。従って、前記記憶手段だけを前記ユーザ携帯端末から脱離させておくことにより、第三者が該端末を使って個人情報を盗用する危険性を殆どなくすることができる。前記記憶手段の所有者は、前記記憶手段を他のユーザ携帯端末に適用して該他のユーザ携帯端末を利用することもできる。

【0025】好ましくは、前記第2の暗号は、前記第1の暗号と同一の暗号方式によるものであり、前記ユーザ携帯端末から受信した前記第1の暗号による暗号化個人情報は、前記認証サーバにおいて復号化されることなく、そのまま前記決済サーバに送信される。

【0026】かかる発明によれば、前記認証サーバにおいて、前記個人情報は暗号化された状態のまま前記決済サーバに送信される。従って、前記認証サーバにおいて、前記個人情報が盗視されたり漏洩したりする危険性がなくなり、より確実にセキュリティが確保される。

【0027】

【発明の実施の形態】以下、添付図面を参照しつつ、本発明の実施の形態について説明する。尚、以下の説明において、「個人ユーザ」とは一般消費者としての個人を念頭においているが、グループや組織であってよい。また、「携帯電話の保有者である個人ユーザは、」という表現を「携帯電話は、」のように簡略に記載することがある。

【0028】実施形態1

図1は、本発明の一実施形態に係る決済システム80の構成を示す概念的ブロック図であり、図2は、該決済システム80において用いる携帯電話の一例を示す概略図である。図1及び図2において、10(10a~10c)はインターネット接続可能なユーザ携帯端末の例としての携帯電話(以下、単に携帯電話という)、15は記憶手段、20はインターネット、30は認証サーバ、40は決済サーバ、50は電子ショップを示す。

【0029】本発明に係る決済システム80は、インターネット20を介して携帯電話10に接続された認証サーバ30を備え、この認証サーバ30はインターネット20を介して決済サーバ40に接続されている。

【0030】かかる決済システム80において、認証サーバ30は、予め、例えば個人ユーザと認証サーバ30の運営者との間でのインターネット上の商取引実施等に関する契約時点等に、携帯電話10から個人情報を送信させ、当該個人情報を、第1の暗号により暗号化して携帯電話10に返信して記憶させておく。

【0031】さらに、認証サーバ30は、携帯電話10からインターネットを介した商取引が行なわれようとする場合に、前記第1の暗号による暗号化個人情報を認証サーバ30に送信させ、該情報を受信したのち復号化

し、第2の暗号により暗号化し、当該第2の暗号による暗号化個人情報を決済サーバ40に送信する。

【0032】以下、本実施形態に係る決済システム80を詳細に説明する。図3は、個人情報の暗号化に関するフローチャート、図4は、発注から決済に至る流れに関するフローチャートをそれぞれ示す。図3及び図4における「端末」は携帯電話10を意味する。

【0033】携帯電話10はユーザ携帯端末の一例であり、インターネット20に接続可能な構成であるとともに、認証サーバ30によって暗号化された個人情報を記憶していることができる構成のものが用いられ、インターネット20上で電子ショップ50との間で情報交換や商取引等を行なうことができる。ここで、ユーザ携帯端末としては、いわゆる「モバイルコンピュータ」のような携帯情報端末、或いは、インターネットに接続可能なPC端末等を含む。また、商取引とは、商品やサービスの内容を吟味したり、購入や契約を手軽に行なったりすること等を含む意味である。

【0034】本実施形態において用いられる携帯電話10は、記憶手段15を備えており、該記憶手段15は、携帯電話10本体に装着又は挿入等によって着脱自在であり且つ直接携帯電話10に電気的に接続することができる。かかる記憶手段15を着脱自在とすべく、携帯電話10本体は、記憶手段15の装着又は挿入ができる記憶手段装着部11a(図2)が配設されるとともに、記憶手段15に対して読取及び書込等を可能とする手段(図示せず)を備えている。

【0035】また、携帯電話10は、①暗号化された個人情報が認証サーバ30から送信されると、当該個人情報を記憶する(図3、ステップ305)、②携帯電話10の行なう商取引に関して認証サーバ30から要求されると、当該個人情報を認証サーバ宛て送信する(図4、ステップ404)、ように処理内容がプログラム化されている。

【0036】このような記憶手段15としては、近年の技術進歩により掌中に収まるような大きさになった携帯電話10に取付可能な、小型で大容量を有する記憶媒体が実現されてきており、その例としては、いわゆる、スマートメディア、コンパクトフラッシュ、メモリスティック、PCカード、MOデノスク、フロッピーディスク等を挙げることができる。

【0037】このような、着脱自在な記憶手段15を用いる構成によれば、暗号化個人情報を記憶手段15に予め記憶させておいて、記憶手段15の利用の有無によって記憶手段15を任意に着脱できるので、利用のないとき記憶手段15だけを携帯電話10から脱離させておけば、インターネットやパソコンからこの記憶手段15にアクセスできない状態を維持できることになる。

【0038】従って、携帯電話10から脱離させた状態では、記憶された個人情報は外部から覗かれ得ない。か

かる記憶手段15は、インターネットやパソコンを利用して第三者が携帯電話10を使って個人情報を盗用する危険性を殆どなくすることができる。

【0039】さらに、記憶手段15の所有者は、記憶手段15を、記憶手段15の装着又は挿入の形態や電気的信号の送受信の形態等に支障の無い限り、他の携帯電話に適用し、その他の携帯電話を利用することもできる。

【0040】記憶手段15は、着脱自在のものをを用いると以上に説明したような利点があるが、或いは、記憶手段15は、携帯電話10に内蔵のものであってもよく、また特段の単独の記憶手段でなくとも、内部のメモリエリア等を利用してよい。

【0041】認証サーバ30は、(1)携帯電話10を保有する個人ユーザの個人認証情報及びカード情報等を含む個人情報を携帯電話10から認証サーバ30を介して決済サーバ40に送信する機能を有する他、(2)当該個人情報を予め暗号化する機能を有する。認証サーバ30は、暗号化に関する所要の手段及び機能を具備している。

【0042】認証サーバ30が個人情報を決済サーバ40に送信する機能(前記(1)の項)を説明する。携帯電話10の個人ユーザと電子ショップ50との間で商取引が開始された場合(ステップ401)、まず、①認証サーバ30は、電子ショップ50から商取引の発注を受けて認証が要求される(ステップ402)ので、携帯電話10に内容確認(ステップ403)させたのち要求して第1の暗号による暗号化個人情報を認証サーバ30に送信させる(ステップ404)。

【0043】次に、認証サーバ30は、②当該暗号化個人情報を受信したのち復号化し、復号化された個人情報を第2の暗号により暗号化し、当該第2の暗号による暗号化個人情報を決済サーバ40に送信する(ステップ405)。従って、認証サーバ30が個人情報を決済サーバ40に送信する機能は、①及び②という2段階の処理内容である。

【0044】実際には、電子ショップ50から商取引の照会があったのち、認証サーバ30は、携帯電話10に前記商取引に関する金額や数量等の内容を確認(ステップ403)させたのち、携帯電話10の個人ユーザが、この商取引を是認したら(ステップ404)、是認である旨として携帯電話の個人認証情報を認証サーバ30に送らせることができる。

【0045】第1及び第2の暗号は、本実施形態においては、公開鍵方式による互いに異なる暗号が用いられる。本実施形態は、第1及び第2の2つの暗号を採用するので例えば、第1の暗号を現在の技術による携帯電話10に採用しやすい暗号方式を設定することができる。第1及び第2の暗号は、公開鍵方式以外の暗号であってもよい。

【0046】個人認証情報としては、本実施形態におい

ては携帯電話のPIN番号が用いられる。携帯電話10が、この個人認証情報を送信する際、認証サーバの要求により、あわせて第1の暗号による暗号化個人情報を認証サーバ30に送信する(ステップ404)。

【0047】また、認証サーバ30は、前述したように、個人情報を予め暗号化する機能(前記(1)の項)を有している。この暗号化機能は、携帯電話が本格的に使用される前に予め、即ち、前述したように、個人ユーザと認証サーバ30の運営者との間でインターネット上の商取引実施等に関する契約がなされた場合等に行なわれる。

【0048】図3に示したように、まず、記憶手段15が携帯電話10に装着され(ステップ301)、携帯電話10が認証サーバ30に接続され(ステップ302)、携帯電話10を介して認証サーバ30に個人情報が入力されたら(ステップ303)、認証サーバ30は、これを第1の暗号により暗号化し(ステップ304)、携帯電話10に送信して記憶させる(ステップ305)。

【0049】認証サーバ30には、以上説明した一連の処理機能(ステップ403～405)及び暗号化機能(ステップ301～305)を実行する手順がコンピュータプログラム化されて記憶されている。また、認証サーバ30は、第1及び第2の暗号方式に関する暗号化及び復号化手段及び機能を有している。

【0050】決済サーバ40は、第2の暗号による暗号化個人情報を復号化し、復号化された個人情報を認証(ステップ406)したのち、認証サーバ30を介して発注先の電子ショップ50に対して前記商取引を承認して実行させる(ステップ407)とともに前記商取引の代金を決済する(ステップ409)。尚、決済のステップ409は、ステップ406より以後であれば随時実行される。

【0051】従って、決済サーバ40は、第2の暗号方式に関する復号化手段及び機能を有しており、決済サーバ40には、以上説明した一連の処理機能及び暗号復号化機能を実行する手順がコンピュータプログラム化されて記憶されている。かかる決済サーバ40は、銀行や信販会社等によって運営され得る。

【0052】電子ショップ50は、ステップ402によって認証サーバ30に商取引の認証を要求し、ステップ408によって携帯電話10に商取引を実行する。前記認証の要求に対しては、認証サーバ30からステップ407によって商取引実行が認められ、商取引の実行に対しては、決済サーバ40から決済を受ける。本明細書において電子ショップとは、かかる商取引のできるサーバ等を意味する。

【0053】このように決済システム80を構成したので、携帯電話10の保有者たる個人ユーザは、発注先の電子ショップ50等に商取引の発注をすると、携帯電話10に記憶された暗号化個人情報を認証サーバ30から

要求されて送信するので、暗号化個人情報を携帯電話 10 に改めて入力する必要が生じるわけではない。同時に、携帯電話 10 には第 1 の暗号による暗号化個人情報が記憶されており、該個人情報は第三者には容易に解読され得ない。

【0054】一方、携帯電話 10 から認証サーバ 30 へ、認証サーバ 30 から決済サーバ 40 へ送受信される個人情報は、それぞれ第 1、第 2 の暗号によってそれぞれ暗号化されているとともに、認証サーバ 30 において、第 1 の暗号による暗号化個人情報が復号化されるが、直ちに第 2 の暗号により暗号化されるので個人情報がハードディスク等の記憶媒体に保存されたりすることはない。結局、個人情報は、認証サーバ 30 に残らず、しかも商取引の発注から決済までのプロセスがすべてインターネット 20 上で行なえるということになる。

【0055】従って、個人ユーザは、暗号化された複雑な個人情報を入力する必要がないので携帯電話 10 の操作が楽で操作性がよく、しかも携帯電話 10 の個人情報のセキュリティが保たれている。

【0056】さらに、認証サーバ 30 に個人情報が残らず、従って、認証サーバ 30 上で個人情報が漏洩するリスクが、従来のように個人情報がファイルされる場合よりも低減でき、前述した暗号方式によりインターネット 20 上における個人情報の送受信に対するセキュリティも確保されている。従って、個人ユーザにとってインターネット 20 上での商取引及び決済が安心且つ便利なものとできる。

【0057】本実施形態は、個人情報が認証サーバ 30 に残らないので、従来、決済サーバ 40 の運営者らが認証サーバ 30 の運営者に対して要望したセキュリティ確保の姿に一步近づくことができる。そして、第 2 の暗号は、決済サーバ 40 が主体的に決定することができるので、例えば、携帯電話 10 によって技術的に利用が困難な暗号方式を用いたい場合等であっても本システムを利用できる。

【0058】実施形態 2

認証サーバ 30 の運営者としては、例えば、決済サーバ 40 の運営者の承認を得ることができれば、第 2 の暗号

を第 1 の暗号と同一のものに設定することができる。実施形態 2 は、第 2 の暗号を第 1 の暗号と同一のものとした構成である。以下、実施形態 2 について、実施形態 1 と異なる点のみ説明する。

【0059】前述のように第 2 の暗号を第 1 の暗号と同一に設定すると、携帯電話 10 から受信した第 1 の暗号による暗号化個人情報は、認証サーバ 30 において復号化される必要はなく、そのまま決済サーバ 40 に送信される。

【0060】従って、認証サーバ 30 において、前記個人情報は暗号化された状態のまま決済サーバ 40 に送信されることとなり、認証サーバ 30 において暗号が解読されることがないので、前記個人情報が盗視されたり漏洩したりする危険性がなくなり、より確実にセキュリティが確保される。従って、本実施形態は、従来、決済サーバ 40 の運営者らが認証サーバ 30 の運営者に対して要望したセキュリティ確保の姿にさらに近づくことができる。

【0061】

【発明の効果】本発明に係る決済システムは、インターネット上で個人情報に対するセキュリティを充分確保できるとともにユーザ携帯端末の操作性をよくし、さらに、商取引から決済に至るプロセスをインターネットのみを利用して一貫して完結できるとともに個人情報を保存するリスクを軽減できる。

【図面の簡単な説明】

【図 1】 本発明の一実施形態に係る決済システムの構成を概略的に示すブロック図。

【図 2】 本発明の一実施形態に係る携帯電話の例を示す概略図。

【図 3】 本発明の一実施形態に係る個人情報の暗号化に関するフローチャート。

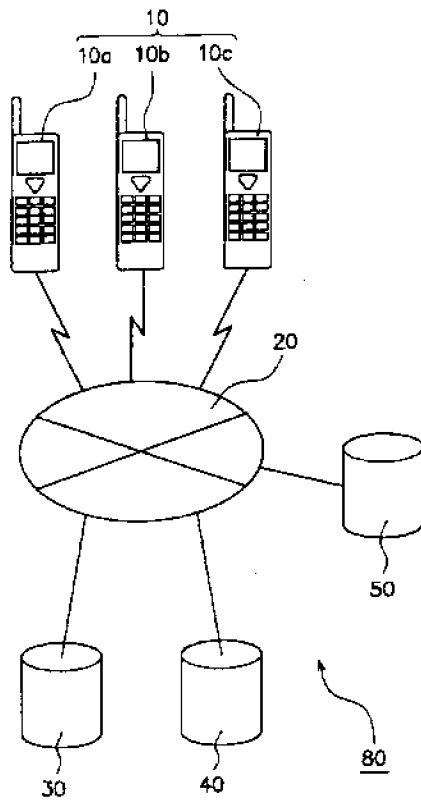
【図 4】 本発明の一実施形態に係る決済システムにおける発注から決済の流れに関するフローチャート。

【符号の説明】

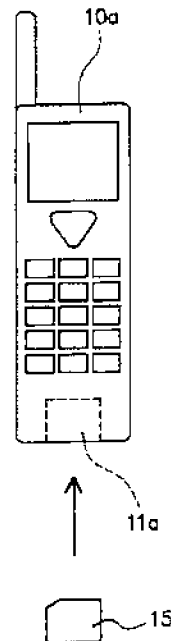
10…携帯電話、20…インターネット、30…認証サーバ、40…決済サーバ、50…電子ショップ



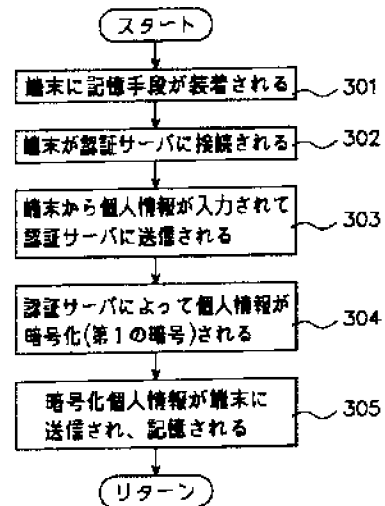
【図 1】



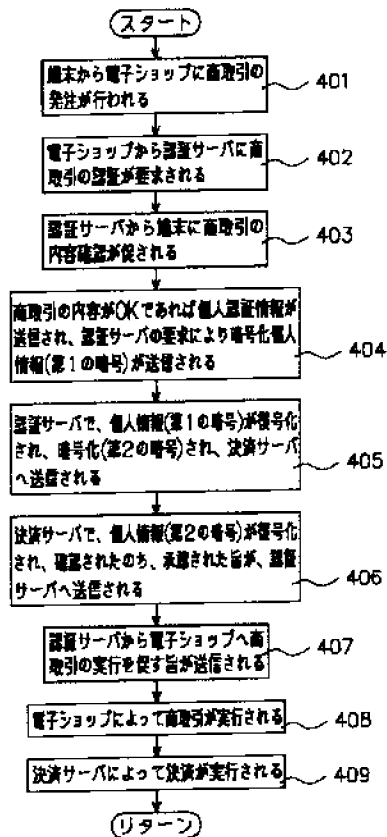
【図 2】



【図 3】



【図 4】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

識別記号

F I  
H 0 4 L 9/00

4-22-1 (参考)

6 7 3 C